TRIBUNAL REGIONAL ELEITORAL DO ACRE

INSTRUÇÃO NORMATIVA Nº 29, DE 22 SETEMBRO DE 2017

Dispõe sobre o os procedimentos para o tratamento e resposta a incidentes em redes computacionais no âmbito do TRE/AC.

A PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ACRE, no uso das atribuições conferidas pelo art. 19, LV e LVII, do Regimento Interno (Resolução nº 1.720, de 16 de junho de 2017),

CONSIDERANDO a Política Corporativa de Segurança da Informação e Comunicação da Justiça Eleitoral (PSI-JE), aprovada pela Resolução TSE nº 23.501, de 19 de dezembro de 2016;

CONSIDERANDO a Política de Segurança da Informação – PSI da Justiça Eleitoral do Acre, instituída por meio da Resolução TRE/AC N. 1.716, de 5 de maio de 2017;

CONSIDERANDO o disposto nos acórdãos TCU n. 866/2011, 594/2011, 7.312/2010 e 2.746/2010 - Plenário, que determinaram a instituição de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à proteção da informação preconizadas pelas normas ISO NBR/IEC 27001:2013 e 27002:2013;

CONSIDERANDO a NC 05/IN01/DSIC/GSIPR, de 04 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta;

CONSIDERANDO a NC 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010, que disciplina a gestão da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, fornecendo diretrizes para o gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal,

RESOLVE:

Art. 1º Estabelecer a política de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do Tribunal Regional Eleitoral do Acre.

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os efeitos desta Instrução Normativa e de suas regulamentações, aplicam-se as seguintes definições:

I - agente responsável: servidor público, ocupante de cargo efetivo do TRE/AC, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

II - artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

III - comunidade ou público alvo: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

IV - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

V - detecção de intrusão: serviço que consiste na análise do tráfego de redes e de histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta a incidentes de segurança em redes computacionais, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão;

VI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - serviço: conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da ETIR;

VIII - tratamento de artefatos maliciosos: serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa;

IX - tratamento de incidentes de segurança em redes computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

X - tratamento de vulnerabilidades: serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em *hardware* ou *software*, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.

DA MISSÃO

Art. 3º A ETIR do Tribunal Regional Eleitoral do Acre terá como missão planejar, coordenar e executar atividades de tratamento e resposta a incidentes de segurança da informação, atuando também de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio do Tribunal.

DO PÚBLICO ALVO

Art. 4º A ETIR terá como público alvo todos os usuários da rede de computadores e de sistemas do TRE/AC, no âmbito da Secretaria do Tribunal e das Zonas e Postos Eleitorais.

Art. 5º Externamente, poderá a ETIR interagir com outros órgãos da Administração Pública Federal, do Poder Legislativo, do Poder Judiciário e do Ministério Público que atuem no mesmo campo da ETIR, fornecendo informações acerca dos incidentes de segurança ocorridos na rede de computadores do TRE/AC, alimentando as suas bases de conhecimentos e fomentando a troca de tecnologias.

Paragrafo único. A comunicação dos incidentes de segurança, bem como o tratamento aplicado, será efetuada através de documento formal.

DO MODELO DE IMPLEMENTAÇÃO

Art. 6º A ETIR será implementada segundo o Modelo 1 da NC 05/IN01/DSIC/GSIPR, devendo ser formada, preferencialmente, por servidores efetivos da Secretaria de Tecnologia da Informação, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

DA AUTONOMIA

Art. 7º A ETIR seguirá o modelo “Autonomia Compartilhada”, descrito no subitem 9.2 da NC 05/IN01/DSIC/GSIPR, que lhe permitirá trabalhar em acordo com outras unidades do Tribunal a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas.

§1º. A ETIR participará no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório. Neste caso, a Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com a unidade a que está hierarquicamente vinculada.

§2º. Quando a ocorrência de um incidente exigir atuação imediata e emergencial, em função de evento crítico confirmado, relacionado à segurança dos sistemas de computação ou das redes de computadores, a ETIR poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

§3º. A ETIR também poderá atuar sem esperar pela aprovação de níveis superiores de gestão nos casos em que o incidente registrado seja de simples resolução e não impacte a instituição como um todo.

§4º. Todos os demais procedimentos ou medidas de recuperação a incidentes em redes computacionais que não se enquadrem no descrito nos parágrafos 2º e 3º deste artigo deverão ser submetidos à aprovação de níveis superiores de gestão.

DA ESTRUTURA ORGANIZACIONAL

Art. 8º A ETIR estará vinculada hierarquicamente à Secretaria de Tecnologia da Informação, que constituirá o primeiro nível de gestão superior. Para os casos mais críticos e complexos, a Diretoria-Geral participará do processo decisório e será considerada o segundo nível de gestão superior. A ETIR, portanto, compartilhará com os níveis superiores de gestão a autonomia para desenvolver suas atividades, submetendo as medidas e ações a serem executadas para resolver os incidentes de segurança à aprovação superior, sempre que necessário, de acordo com o estipulado no Art. 7º desta Instrução Normativa.

Art. 9º Mensalmente, a ETIR deverá apresentar à Comissão de Segurança da Informação relatórios estatísticos dos incidentes de segurança ocorridos no período, com os respectivos tratamentos adotados, com vistas à elaboração de estudos de melhoria dos mecanismos de segurança estabelecidos no Tribunal ou para fins de tomada de decisão estratégica relativa à Segurança da Informação junto à Administração.

Art. 10. A ETIR será formada, preferencialmente, por servidores públicos efetivos lotados na área de Infraestrutura de Rede de Computadores do Tribunal.

§ 1º Para cada integrante titular, será indicado o respectivo substituto.

§ 2º Seus integrantes, titulares e substitutos, serão indicados pelo Secretário de Tecnologia da Informação, e designados por meio de Portaria da Diretoria-Geral.

§ 3º Dentre os titulares, um deverá ser indicado como Agente Responsável.

Art. 11. A ETIR funcionará como um grupo de trabalho permanente, de atuação primordialmente reativa e não exclusiva.

Parágrafo único. As atividades reativas da ETIR terão prioridade sobre aquelas designadas pelos chefes imediatos de seus respectivos integrantes.

DOS SERVIÇOS E PROCEDIMENTOS

Art. 12. São serviços a serem implementados e desempenhados pela ETIR:

I - tratamento de incidentes de segurança em redes computacionais;

II - tratamento de artefatos maliciosos;

III - tratamento de vulnerabilidades;

IV - monitoramento da segurança da rede de computadores.

Art. 13. Para cada serviço elencado no artigo anterior, deverão ser formalizados procedimentos a serem observados pela ETIR, em documento a ser elaborado pelo Agente Responsável, com o apoio de toda a equipe, contendo os seguintes atributos:

I - a definição do serviço;

II - o objetivo do serviço;

III - a descrição das funções e procedimentos que compõem o serviço.

Parágrafo único. O documento de que trata este artigo deverá ser elaborado pela Equipe, após sua nomeação, no prazo máximo de 6 (seis) meses, e atualizado sempre que necessário.

DAS RESPONSABILIDADES

Art. 14. Caberá ao Agente Responsável:

I - elaborar os procedimentos internos a serem observados pela ETIR, com apoio da própria equipe;

II - gerenciar as atividades desempenhadas pela ETIR;

III - distribuir, sempre que necessário, tarefas para a ETIR, inclusive as de caráter pró-ativo;

IV - sugerir ao Secretário de Tecnologia da Informação, quando necessário, a convocação de representantes de outras unidades da Secretaria de Tecnologia da Informação, para atuar no tratamento e resposta de determinado incidente de segurança;

V - treinar integrantes da equipe, para o fiel desempenho de suas atividades;

VI - assegurar que os usuários sejam informados sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados;

VII - cuidar para a manutenção da capacitação dos membros da ETIR, fazendo constar do Plano Anual de Capacitação os eventos que entender relevantes ao bom desempenho dos trabalhos da equipe.

Art. 15. Caberá à ETIR:

I - manter registro dos incidentes de segurança em redes de computadores notificados ou detectados, com o objetivo de assegurar registro histórico das atividades da ETIR;

II- recolher evidências imediatamente após a constatação de um incidente de segurança da informação na rede interna de computadores;

III - executar análise crítica sobre os registros de falha para assegurar que as mesmas foram satisfatoriamente resolvidas;

IV - investigar as causas dos incidentes de segurança da informação na rede interna de computadores;

V - implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

VI - indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e

o custo de futuras ocorrências de incidentes.

Art. 16. Caberá ao Secretário de Tecnologia da Informação:

I - submeter ao Diretor Geral a indicação do Agente Responsável, dos servidores titulares da ETIR e seus respectivos substitutos;

II - apoiar a ETIR, na execução de seu trabalho, viabilizando a disponibilização dos recursos materiais, tecnológicos e humanos necessários à prestação dos serviços oferecidos aos usuários;

III - participar do processo decisório como primeiro nível de gestão superior, decidindo as questões submetidas pela ETIR de acordo com a criticidade e complexidade de cada caso.

Art. 17. Caberá ao Diretor Geral:

I - expedir portaria nomeando o Agente Responsável, os servidores titulares da ETIR e seus respectivos substitutos;

II - participar do processo decisório como segundo nível de gestão superior, decidindo as questões submetidas pela Secretaria de Tecnologia da Informação de acordo com o impacto à continuidade do negócio do Tribunal.

DAS DISPOSIÇÕES GERAIS

Art. 18. Os casos omissos e as dúvidas surgidas na aplicação desta Instrução Normativa serão dirimidos pela Comissão de Segurança da Informação deste Tribunal.

Art. 19. Este normativo deverá ser revisado periodicamente, em intervalos de, no máximo, três anos.

Art. 20. No prazo de 10 dias, o Tribunal deverá nomear os integrantes da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, titulares e respectivos substitutos, observado o disposto nesta Instrução Normativa.

Art. 21. Esta Instrução Normativa entra em vigor na data de sua publicação.

Rio Branco, 22 de setembro de 2017.

Documento assinado eletronicamente por **Regina Célia Ferrari Longuini**, **Presidente**, em 27/11/2017, às 15:39, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ac.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0166012** e o código CRC **9F7D994D**.